SHARED APPLICATION SOFTWARE REVIEW PROGRAM

CHAPTER 7

(FILE NAME ON DISK # 1 = S1C7.WPD)

The SASR Program was established in 1990 by the FFIEC IS Subcommittee and is structured similarly to the successful interagency sponsored Shared National Credit Program (SNC). Under SNC large multinational/ regional credit lines, with participation across interagency jurisdictions, are reviewed by interagency groups of credit review examiners annually. In the same fashion, interagency IS examiner resources are used to review and evaluate uniformly the control structure of major software packages used by a wide segment of financial institutions. Normally, a software/turnkey program or system would be used by financial institutions across agency supervisory jurisdictions, leading to cross-agency involvement.

The scope of the SASR program covers: turnkey systems (which generally include an integrated mix of both software and hardware), stand-alone custom software (which runs on a commercially standard hardware configuration), and integrated packages. Criteria for selection includes purchased software that involves high risk applications. These applications were envisioned to include wire transfer, securities transfer, loans, deposits, and general ledger.

SASR PROGRAM

The FFIEC IS Subcommittee believes the primary focus of the SASR program is the review of turnkey software packages used by financial institutions. The benefits of the program include:

- A more cost effective use of agency/interagency IS examiner resources.
- Providing agencies with the expertise to review these systems and applications jointly.
- The ability of each agency to use non-speciality more junior safety and soundness examiners or newer IS examiners who understand a community bank’s IS related operational and internal controls. (These examiners generally are not trained to evaluate systems development and programming activities. However, a well-documented SASR report will provide examiners with guidance and assistance to evaluate the small bank IS environment.)

The use of SASR is not limited to the review of community financial institution turnkey systems. It can also be used to support interagency safety and soundness initiatives when focusing on higher risk applications in larger financial institutions. It may be used to evaluate financial institution software packages for wire transfer, capital markets, derivatives development/recordkeeping, securities transfer, and trust transactions.

OBJECTIVES

The SASR program is intended to:

- Augment the IS work in community banks, particularly in systems development and programming.
- Communicate an evaluation that can be used to reduce time and resources needed to examine turnkey facilities.
- Reach conclusions on the adequacy of the software product and whether it is safe, sound, and appropriate for use in a large group of financial institutions.
- Consider systemic risk by targeting software used by a large number of covered financial institutions.
- Maintain a continuing knowledge of software upgrades and changes.

RESPONSIBILITY

The IS Subcommittee of the FFIEC's Task Force on Supervision is responsible ultimately for overseeing the SASR program. This includes choosing software systems for review and selection by the lead agency. Because of the continuing demand by all agencies for senior IS examiner resources, the performance of SASR evaluations must be clearly beneficial when comparing the costs with the benefits.

ADMINISTRATION

The selection of candidates for this program are turnkey (complete software and hardware systems), stand alone software, and integrated packages. Criteria for selection also includes purchased software that involves high risk applications. Such applications include wire transfer, securities transfer, loans, deposits, and general ledger.

The IS Subcommittee of the FFIEC's Task Force on Supervision oversees the program and selects the software system for lead agency review.

A designated lead agency conducts the review in an institution that it supervises. The review should be preceded by the regular IS examination to ensure that the institution is fully prepared for the review team.
The lead agency also performs:

- Examiner-in-Charge Selection – An experienced IS examiner should be selected to head the review.

- Notification – The lead agency must provide other agencies with at least six months prior notice of the upcoming review to assure the availability of senior IS examiners.

- Research – The lead agency must perform preliminary research of the selected software product before beginning the review. The research information must include background data and a description of the organizational structure of the firm and any user group activity. Information collected before the review aids in setting its scope. (An Examiner Checklist is included with this material.)

- Institution Selection – The lead agency selects the institution where the software review will be conducted and notifies the participating agencies of the target review date. (The institution should use all core software applications.)

- Vendor Notification – The lead agency must notify the vendor of the upcoming software review and to designate a contact person. (See sample letters attached.) The vendor may provide information and suggestions that enhance the review. The vendor must be informed that the final product of this review will be a confidential report for regulatory purposes only. A copy of the report will not be made available to either the vendor or any of the user financial institutions. The vendor should be advised that participation in the SASR program should not be publicized and the review should not be construed as an endorsement of the software program.

- Performance Review – The program administration and instruction documents establish guidelines for performing shared application software reviews. The EIC will advise the financial institution and the software vendor that the SASR is intended to provide an in-depth review of the characteristics and features of a particular software product. A confidential report, summarizing the review findings, must be completed for all such reviews and be strictly for regulatory purposes only. No copies will be provided to the financial institution or the software vendor.

- Exit Meeting – An exit meeting must be conducted at the mutual convenience of the vendor and the participating examiners. Ideally a draft report should be available for this meeting with the vendor. The draft report may be discussed with the vendor representative, but must be returned after the meeting to ensure the accuracy of the information developed. In addition, the EIC may request comments on planned enhancements to the software program.

  Significant areas of concern to examiners identified in the review should be discussed during the exit meeting. With the approval of the IS Subcommittee, they may be documented in a follow-up letter to the vendor. If a meeting is impractical, a conference call will suffice.

- Review Submission – All reviews should be completed and forwarded to the Washington, D.C. office of the lead agency within 30 days from the completion of the on-site review. To facilitate the review process, both a hard copy and an electronic version (preferably ASCII) of the review should be provided.

- Document Review and Distribution -- The IS Subcommittee will review and distribute the final product. Each agency will distribute the report to its respective regional office or district. (These documents are for internal agency purposes only.)

Follow-up – The vendor should be requested to keep the lead agency apprised of major software changes and enhancements.

Scheduled Updates — Feedback from field examiners can trigger another review. These events may include a change of ownership, significant software changes, or new developments that adversely affect institutions using the software.

GUIDELINES FOR SASR REPORTS

These guidelines are provided to assist the examiner in conducting Shared Application Software Reviews (SASR). They address the same areas as the FFIEC IS Workprogram. The examiner may review other areas based on the findings. Additionally, the examiner is encouraged to include any relevant information obtained from outside sources. This information should be verified.

The SASR is intended to produce a report documenting the characteristics and features of the selected software product. This will assist examiners in conducting examinations (safety and soundness, compliance, bank holding company inspections and IS) of financial institutions using a specific software product. The scope of the SASR should be flexible to accommodate the changing data processing environment and include, at a minimum, the following information.

A cover sheet should clearly state:

- "SHARED APPLICATION SOFTWARE REVIEW."
- Vendor name and corporate address.
- Software product reviewed.
- "THIS REVIEW IS THE PROPERTY OF THE FFIEC MEMBER AGENCIES AND IS NOT TO BE DUPLICATED WITHOUT PERMISSION. THIS REVIEW IS FOR INTERNAL USE ONLY."

A table of contents should be included.

GENERAL OVERVIEW

Page one of the report consists of a general description of vendor responsibilities. It should contain the following information.

Vendor – Indicate the vendor's name, corporate address, and the name of a contact person.

Date – Indicate the date the software review began.

Application Software System– Describe the software system being reviewed and include the system description and capacity for hardware, software, and telecommunications. Describe:

- The system software requirements.
- The software's capacity by determining the number of accounts, number of transactions, telecommunication speeds, etc.
- The release level(s) of the software product supported by the vendor.
- Hardware requirements to operate the software (include disk and memory requirements).
- The capacity of the storage devices.
- The telecommunications network that includes the applications, hardware, and compatible devices required to operate it.

Type and Number of Users – Indicate the total number of financial institutions using this software by type of institution.

Organizational Structure – Describe briefly the corporate and financial history of the vendor.

User Group Contact – Indicate the user group liaison.

EXAMINER'S CONCLUSIONS

Briefly summarize the significant findings of the report sections, in the following order: Audit, Management, Systems Development and Programming, Operations, and Networking.

INTERNAL/EXTERNAL AUDIT

Audit Software – Determine if the institution uses the audit software included with the software package or another audit program. If another program is used, determine why. Describe audit software if it is included with the software package. Review the documentation provided.

External/Internal Audit – Determine whether the software has been reviewed by internal or external auditors. Note any deficiencies disclosed and determine the necessary follow-up.

MANAGEMENT

Management Staff/Succession – Determine whether the vendor has sufficient staff to maintain the software. Address the depth of staff and provide for adequate management succession.

Training – Comment on the extent of vendor provided training.

User Groups – Ascertain if there are user groups that meet regularly to discuss software deficiencies, future plans, and current topics. Comment on the vendor's responsiveness to the user groups' concerns.

Source Code – Determine whether the vendor provides a source code and program/system documentation or, if not, whether an escrow agreement exists. The related code and documentation should be under the custodianship of a disinterested third party. Determine if the code and documentation are subject to audit and if the frequency of these audits is appropriate.

Costs/Fees – Decide whether vendor costs/fees are reasonable. The examiner should consider upgrade fees, training costs, conversion costs, and other related expenses.

Vendor Support – Determine whether the vendor provides adequate continuous support to meet the needs of the user.

Contact Hotline – Determine whether a technical support contact is available to resolve software problems encountered by the user.

Future Issues – Document the vendor's plans, including future releases and required hardware upgrades.

Accounting Issues – Review vendor provided software accounting guidelines relating to purchase costs and incremental installation/conversion costs and comment on whether they comply with GAAP.

Compliance Methodology – Determine whether the vendor has a regulatory compliance office; how the vendor becomes aware of regulatory changes; and whether the software provides reports that comply with applicable laws and regulations.

Insurance – Provide a description of the vendor's fidelity bond coverage.

Contracts – Review existing contracts between the vendor and user. Determine if the contract conforms with FFIEC guidelines.

SYSTEMS DEVELOPMENT AND PROGRAMMING

Documentation – Determine the quality of the documentation provided and whether it is current. This review should address only vendor provided documentation. However, the examiner should be aware of enhancements created by the user.

Programming Documentation – Determine whether the systems development and programming documentation includes:

- System narrative.
- System flowchart.
- Program narrative.
- Program flowchart.
- Data elements.
- File layouts.
- Descriptions of edits.
- Report layouts.
- Descriptions of tables.
- Current source listings.
- Program change history.
- Other elements considered necessary by the examiner.

Utilities – Identify all data altering utilities. Determine whether the application has its own utilities or relies on operating system utilities. The examiner should identify any other utility programs that affect the control environment and identify applicable controls.

Release Process – Identify the vendor's latest software version and the one at the institution, noting the release and implementation procedures. Indicate the extent to which periodic updates are required, such as year-end updates.

Software Controls – Identify built-in software controls that may include:

- Limit checks.
- Range checks.
- Alpha/numeric checks.
- Reasonableness checks.
- Check digit tests.
- Run-to-run totals.
- Date checks.
- Hash totals.
- Batch totals.
- Tests for zero/blank fields.
- Test for mathematical sign.
- Field and code value checks.
- Edit tests.

System Requirements – Determine the system software requirements and the required resources.

Software Capacity – Analyze the software's capacity by determining the number of accounts, number of transactions, telecommunication speeds, etc.

Audit Trail – Determine whether audit trails are in place to trace and record all transactions. All transactions should be listed on a transaction register and all exception transactions noted on an error/suspense report.

Systems Development Life Cycle (SDLC) – Determine if an SDLC methodology is used by the vendor. Comment on the level of user involvement throughout the SDLC process and the effectiveness of user participation. (See Chapter 9 Systems Development Life Cycle and Waterfall System Development.)

Programming Languages – Describe the programming language used by the vendor to maintain the software. Determine whether it is currently being supported by the vendor. Also comment on the vendor's ability to maintain it. Determine if the size and depth of the programming staff is adequate relative to the programming backlog and projects under development.

Software/Hardware Interface – Determine whether the software:

- Interfaces with other software products.

- Is limited to products offered by that vendor.

- From another vendor which has been added, violates the licensing contract.

Program Maintenance – Describe the process for performing program maintenance. Determine the utility programs necessary to install program changes. Determine how new releases are moved into production.

Software Maintenance (Vendor Supplied) – Determine whether the vendor provides program maintenance. If so, determine what procedures are in place to handle these changes and current documentation is provided with each update. Comment on the adequacy of vendor testing.

DATA INTEGRITY

File Maintenance – Identify how file maintenance is performed by answering the following questions: Can the user perform file maintenance on all files and fields within each record? Which fields are locked out? Who is authorized to perform file maintenance? Is knowledge of a programming language required? If so, which ones? Are procedures well documented? What type of security is in place for this process? (See Chapter 14.)

Output Reports – Determine whether the reports meet the user's needs. Are they easy to read and understand? Does each report have a specific heading or title page? Does the software include report writer capabilities?

Input Controls – Identify software input controls. Address controls for error checking, input validation, and supervisory overrides.

Input/Output Balancing – Review the user's manual for instructions and examples on how to reconcile various reports. Additionally, note whether the instructions are concise and clear.

Error Exceptions – Review the vendor provided documentation and determine whether there are error and edit routines for all critical fields. Review the type of error and exception reports that are provided and whether they are adequate. Ensure that the exception report shows a before and after correction and states the problem and how to correct it.

OPERATIONS

Hardware Capacity – Determine the number of accounts that can be processed by the system and the transaction capacity of the software. Determine if the file size and transaction volumes are monitored to ensure that users are aware of hardware/software utilization.

Utilities – Identify utility programs that have the ability to alter or destroy data and program files. Describe the controls in place to monitor usage.

Restart/Recovery – For selected applications, identify the vendor provided restart/recovery procedures. Determine whether the processing can be restarted without returning to the previous days work.

Documentation – Review the quality of operator and user documentation. Note whether the documentation provides clear instructions to the user.

Backup – Identify the procedures necessary to backup program and data files, including master and transaction files.

Logging – Decide whether hardware features provide for an audit trail of system functions through a console log. Describe logging procedures.

Operating Systems – Decide whether the software vendor provides operating system maintenance.

Contingency Planning – If contingency planning is provided by the vendor, determine the adequacy of the plan, whether it complies with FFIEC policy, and whether it:

- Has been tested periodically, with results reported to the board of directors or designated committee.

- Is comprehensive.

- Addresses telecommunications.

- Provides for all hardware in place at the backup site and is compatible.

Performance – Determine whether there are system characteristics that could impede performance and telecommunications response time.

Maintenance Agreements – Note whether hardware maintenance is included in the software contract, if leased from the vendor.

NETWORKING AND CLIENT/SERVER

Description – Provide a general description of the telecommunication network, including the applications, hardware, and compatible devices required to operate. Identify the devices the system can support.

Data Security – Identify the security system in place to protect the network and related applications. Determine whether it provides the user with the ability to implement levels of security by user or application and provides CRT lockout and time-out capabilities. Verify whether the security package is vendor supplied or an independent package. Describe security reports available.

EXAMINATION AIDS

Description – Determine if a report generator option is available to the users. Provide any information on software capabilities or reports that may facilitate examination efforts of institutions (including IS, safety and soundness, trust, bank holding company, or compliance examinations, or financial institution liquidations) that use this software program. The examiner should list and briefly describe these reports.

Microcomputers – Indicate whether the vendor provides the capability to upload and download information to and from microcomputer files.

ADMINISTRATION SECTION

Description – Prepare a recap of program participants, indicating name, agency, and examiner hours on the job. Also provide any information that may be of assistance when scheduling a subsequent review of this software product, such as contacts.

Future Plans – Discuss the future plans of the vendor.

User List – Provide a list of user institutions using the software product being reviewed.

Turnkey Workprogram – Provide responses to the Systems and Programming (see Chapter 12) and any other applicable section of the FFIEC Community Financial Institution IS Workprogram (see Chapter 23 - Community Financial Institution Examination Program).

SHARED APPLICATION SOFTWARE REVIEW CHECKLIST

OFF-SITE

_____ 1) Send notification letters to the corporate headquarters of the vendor selected for review and the financial institution at which the review is to be conducted.

_____ 2) Perform background research on vendor. Information to be obtained from the vendor to assist the examiner-in-charge should include:
- User list by type of financial institution.
- User group information.
- List of vendor software manuals provided with the software package.
- Copy of standard software contract or licensing agreement.
- Copy of vendor insurance coverage.
- Information pertaining to the vendor's future plans.
- Vendor's latest annual financial statement or annual report.

_____ 3) Prepare an information package for examiners participating in the shared application software review. Materials to be included:
- Name and address of vendor.
- Name and address of financial institution where the review is being conducted.
- Contact person at the financial institution and vendor.
- Location, time and date review is scheduled to begin.
- Vendor profile (include a brief corporate history and organizational structure).

_____ 4) Send information package to examiners scheduled to participate in the review.

ON-SITE

_____ 5) Conduct a brief meeting with data center management, including vendor if on-site, to reiterate the purpose of the review.

_____ 6) Discuss assignments with participating examiners.

_____ 7) Select applications for detailed documentation review.

_____ 8) Make arrangements for an exit meeting with the vendor.

_____ 9) Submit a final written review, along with an electronic version, to the lead agency's Washington, D.C. office for final review and distribution.

SAMPLE INSTITUTION NOTIFICATION LETTER

<Date>

<Name>
<Title>
<Financial Institution>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to inform you that a software review of <software product> is scheduled to take place at your bank commencing <date>. The review is scheduled to take approximately two weeks and will follow the regularly scheduled IS examination of your data center. The <agency name> is in charge of the software review and will be assisted by representatives from the <name participating agencies>. The software vendor has been requested to provide support for this review.

In brief, the Federal Financial Institutions Examination Council has instituted a Shared Application Software Review (SASR) program to review "turnkey" software programs which are widely used by insured depository institutions. This program is designed to assist the federal regulators in developing more consistent examinations of data centers using "turnkey" software and to more efficiently use examiner resources. The review is intended to report the characteristics of the software program such as: operating environment, output reports, audit and control features, upgrade and maintenance procedures, as well as other information to assist examiners in conducting examinations of data centers using this software product. No rating of the software will be assigned nor should this review be construed as an endorsement of this product. The review report is solely for internal use by the FFIEC member agencies. No report copies will be made available to user institutions or to the vendor.

If you have any questions regarding the upcoming review, please contact <name> at <phone number>.

Sincerely,

<Name>
<Title>

SAMPLE VENDOR NOTIFICATION LETTER

<Date>

<Name>
<Title>
<Corporate Name>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to inform you of an upcoming software review of your <software product>, which is scheduled to take place at <financial institution & location> commencing <date>. In 1991 the Federal Financial Institutions Examination Council (FFIEC) instituted the Shared Application Software Review ("SASR") program wherein the federal regulatory agencies comprising the FFIEC would conduct in-depth reviews of widely used "turnkey" software programs. The reviews are designed to assist federal regulatory agencies in developing more consistent examinations of data centers using this product and to more efficiently use examiner resources. It is intended to report the characteristics of the software program, such as operating environment, output reports, audit and control features, upgrade and maintenance procedures, and other information to assist examiners in conducting examinations of data centers using this software product. No rating will be assigned as a result of this review nor should this review be construed as an endorsement of this product. Although the review will culminate in a report, it is solely for internal use by the FFIEC member agencies. No report copies will be made available to your organization or the user financial institutions. An exit meeting will be scheduled at the conclusion of this review to discuss the overall findings and any concerns, if applicable.

You are encouraged to make available a contact person to whom questions can be addressed. To facilitate the review enclosed is a vendor request list which should be completed and returned to my attention by <date>. Thank you for your assistance and prompt response.

If you have any questions, please contact <name> at <phone number>.

Sincerely,

<Name>
<Title>

Enclosure

SHARED APPLICATION SOFTWARE REVIEW VENDOR REQUEST LIST

To facilitate the review process and to minimize the disruption to your organization, kindly assist us by:

- Providing copies of the latest audit of the company or third-party reviews of the software.
- Describing briefly the corporate and financial history of your firm and providing an organizational chart.
- Listing the companies licensed to sell the <name> software package, including a copy of the franchise or licensing agreement.
- Describing briefly the programming staff supporting the <product name>.
- Describing future software enhancements and planned future releases for the <product name>.
- Describing how your company monitors regulatory changes to ensure that your software product complies with applicable laws and regulations.
- Describing insurance coverage, including fidelity bond and errors and omissions insurance.
- Providing copies of your firm's last three annual reports. If your company does not prepare an annual report, please provide copies of the last three fiscal year-end financial statements and statements of income and expense. Also, include quarterly information to date.
- Providing an overview of the <software> system, as well as the applications it supports.
- Listing the various programming languages used.
- Identifying the release levels of the software that you currently support.
- Providing an overview of the System Development Life Cycle ("SDLC") methodology used by your company. Also, describe what user involvement is employed within your SDLC program.
- Describing the process for performing program maintenance and list the steps the institution would find necessary to install the program changes.
- Describing release information and other maintenance documentation provided the institution as part of the release process.
- Describing software capacity information related to number of accounts, number of transactions and number of institutions that the software will support.
- If the source code is maintained in an escrow agreement, providing..
  - The name and address of the escrow agent.
  - A listing of materials stored with the escrow agent.
  - A description of procedures to ensure that the most current copy of the source code is at the escrow location.
  - A copy of the most recent audit of the escrow storage.
  - A copy of the escrow agreement.

  - A copy of the authorized user list provided to the escrow agent.

- Describing the hardware requirements to operate the software, including disk and memory requirements.

- Detailing the hardware features for logging system activity and whether a facility exists to specifically isolate the usage of sensitive transactions and utilities.

- Listing any software characteristics or conditions which could impede system performance and telecommunications response time.

- Providing a general description of the telecommunications network which includes applications, hardware, and compatible devices to operate. Additionally, list the number of terminals that this system can support.

- Identifying the security system in place to protect the network and related applications. Also, describe the levels of security that the user may implement.

- Providing a customer listing of institutions using the software. The list should include total number of institutions by type (i.e. national, state member, state nonmember, savings and loan, and credit union).

- Describing briefly the initial and continuing education programs offered financial institutions.

- If user groups are maintained, noting how often they meet. Also, describe future plans, product enhancements, and current issues that have been generated by the user group.

- Providing a copy of a blank standard contract/licensing agreement. Indicate standard contract period and renewal options.

- Providing a copy of software accounting guidelines for purchase and incremental installation/conversion costs are provided to your customers.

- Listing other products or services are offered to financial institutions.

- Providing a list of standard and custom reports available to the bank.

- Describing any personal computer activities supported by the software product.

- Describing any report writer packages that are compatible with or supported by this product.

SAMPLE ACKNOWLEDGMENT LETTER

<Date>

<Name>
<Title>
<Corporate Name>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to acknowledge your company's assistance at our review of your firm's <software product> which began <date>. The review was performed by representatives of this office, the <participating agencies> at the <financial institution>. Your staff was most helpful in our efforts to review your <software product> banking system.

The software review program is designed to assess software products at one location to reduce subsequent reviews at other institutions. The final report will assist regulatory examiners in their examinations of financial institutions that use the <software product> software package.

This review will not result in the assignment of a rating. The resulting report from this review is confidential and for the internal use of the participating FFIEC member agencies. Copies of the software review will not be distributed to participating vendors or user institutions. Additionally, vendors are not permitted to disclose the fact that their software products have been reviewed by the FFIEC.

Again, your assistance in this program is appreciated.

Sincerely,

<Name>
<Title>

SAMPLE COVER PAGE

SHARED APPLICATION SOFTWARE REVIEW

____
Software Product Reviewed

____
Software Vendor

____
Vendor Address

____
Date of Review

____
Lead Agency

PARTICIPATING AGENCIES

THIS REPORT IS STRICTLY CONFIDENTIAL
THIS REVIEW IS THE PROPERTY OF THE FFIEC MEMBER AGENCIES AND IS NOT TO BE DUPLICATED WITHOUT PERMISSION. THIS REVIEW IS FOR INTERNAL USE ONLY.

SAMPLE TABLE OF CONTENTS

A table of contents should be provided immediately following the report cover.

Table of Contents

General Overview ....
Examiner’s Conclusions....................................
Internal/External Audit...................................
Management ....
Systems Development and Programming........................
Data Integrity ....
Operations ....
Networking..
Examination Aids ....